WILLIAMS, MORGAN & AMERSON, P.C

10333 Richmond Drive, Suite 1100, Houston, Texas 77042
phone: 713-934-7000 fax: 713-934-7011

FACSIMILE TRANSMITTAL SHEET

DATE:	APRIL 25, 2006		
TO:	Emmanuel L. Moise	TOTAL NO. OF PAGES INCLUDING COVER:	28
FAX:	1-571-272-3793		
FROM:	MARK W. SINCELL	PHONE:	(713) 934-4052
RE:	RESPONSE TO NON-COMPLIANT DATED MAY 20, 2006	FILE:	2000.054000 S/N 09/901,212

□ URGENT □ FOR REVIEW □ PLEASE YOUR FILE □ PLEASE REPLY □ PLEASE HANDLE

ORIGINAL: □ WILL FOLLOW ☑ WILL NOT FOLLOW

NOTES/COMMENTS:

MARK W. SINCELL | Agent
Williams, Morgan & Amerson, P.C.
10333 Richmond | Suite 1100 | Houston, TX 77042
Voice: 713-934-4052| Fax: 713-934-7011
EMAIL: MSINCELL@WMALAW.COM

CONFIDENTIALITY NOTE

The documents accompanying this facsimile transmission contain information from the law firm of Williams, Morgan & Amerson which may be confidential and/or privileged. The information is intended to be for the use of the individual or entity named on this transmission sheet. If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this faxed information is prohibited. If you have received this facsimile in error, please notify us by telephone immediately so that we can arrange for the retrieval of the original documents at no cost to you.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
Geoffrey S. Strongin, et al.

Serial No.: 09/901,212

Filed: July 9, 2001

For: SOFTWARE MODEM WITH PRIVILEGED MODE DRIVER AUTHENTICATION

Examiner: A. Moorthy

Group Art Unit: 2131

Att'y Docket: 2000.054000

Customer No. 023720

APPEAL BRIEF

CERTIFICATE OF MAILING
37 C.F.R. 1.8

I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date below:

4.25.06
Date

Kathy [illegible]
Signature

Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This paper is submitted in response to the Notice of Non-Compliant Amendment dated April 20, 2006, for which the one-month date for response is May 20, 2006.

Appellant hereby submits this Appeal Brief to the Board of Patent Appeals and Interferences in response to the final Office Action dated September 8, 2005. A Notice of Appeal was filed on December 1, 2005 and so this Appeal Brief is believed to be timely filed.

The Assistant Commissioner is authorized to deduct the fee for filing this Appeal Brief ($500) from Advanced Micro Devices, Inc.'s Deposit Account 01-0365/TT4046.[1]

[1] In the event the monies in that account are insufficient, the Director is authorized to withdraw funds from Williams, Morgan & Amerson, P.C. Deposit Account No. 50-0786/2000.054000.

I. REAL PARTY IN INTEREST

The present application is owned by Advanced Micro Devices, Inc. The assignment of the present application to Advanced Micro Devices, Inc., is recorded at Reel 012012, Frame 0960.

II. RELATED APPEALS AND INTERFERENCES

Appellant is not aware of any related appeals and/or interferences that might affect the outcome of this proceeding.

III. STATUS OF THE CLAIMS

Claims 1-41 are pending in the application. Claims 1-2, 5-11, and 14-15 stand rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by Beckert, et al (U.S. Patent No. 5,794,164). Claims 3-4 and 12-13 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Beckert in view of Moore (U.S. Patent No. 5,343,527). Claims 16-17, 20-21, 23-29, and 32-33 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by Jain (U.S. Patent No. 6,367,018). Claims 18-19 and 31 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Jain in view of Moore. Claim 22 stands rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Jain in view of Fleming, et al (U.S. Patent No. 6,212,360). Claim 30 stands rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Jain in view of Moore and further in view of Labatte, et al (U.S. Patent No. 5,901,301). Claims 34-41 stand rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by Scherf (U.S. Patent No. 5,390,301).

IV. STATUS OF AMENDMENTS

There were no amendments after the final rejections.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 sets forth a computer system that includes a peripheral device and a processing unit adapted to execute a driver for interfacing with the peripheral device in a standard mode of operation and an authentication agent in a privileged mode of operation. The authentication agent includes program instructions adapted to authenticate the driver. Claims 2-15 depend from claim 1.

For example, processor complex 110 has two modes of operation, a standard mode and a privileged mode. An exemplary privileged mode of operation, well known to those of ordinary skill in the art, is the System Management Mode (SMM). See Patent Application, page 13, ll. 18-20. The processor complex 110 executes program instructions encoded in a modem driver 240. The processor complex 110 also executes program instructions for implementing the authentication agent 90. See Patent Application, page 15, ll. 6-10. The authentication agent 90 is periodically invoked to verify the authenticity of the modem driver 240. The authentication agent 90 is invoked in a privileged context, such as by executing the authentication agent 90 in SMM, executing the authentication agent 90 using a cryptoprocessor, or executing the authentication agent 90 using a secure extension of the main system microprocessor. See Patent Application, page 16, line 11-15.

Independent claim 16 sets forth a communications system that includes a physical layer hardware unit and a processing unit. The physical layer hardware unit is adapted to communicate data over a communications channel in accordance with assigned transmission parameters. The physical layer hardware unit is also adapted to receive an incoming signal over the communications channel and sample the incoming signal to generate a digital received signal.

The processing unit is adapted to execute a modem driver in a standard mode of operation and an authentication agent in a privileged mode of operation. The standard mode driver includes program instructions adapted to extract control codes from the digital received signal and configure the physical layer hardware assigned transmission parameters based on the control codes. The authentication agent includes program instructions adapted to authenticate the modem driver. Claims 17-33 depend from claim 16.

For example, processor complex 110 is coupled to a peripheral bus 120, such as a peripheral component interface (PCI) bus, which hosts the hardware portion of a software modem 50. The software modem 50 includes a PHY hardware unit 220 and a radio 230. In the illustrated embodiment, the radio 230 is adapted to transmit and receive GSM signals. See Patent Application, page 14, line 14 – page 15, line 5. Time slot and frequency assignments to for incoming data may be communicated to the software modem 50. Collectively, the time slot, frequency, and power level (*i.e.*, for transmit data only) assignments are referred to as control codes. See Patent Application, page 12, ll. 14-21.

The processor complex 110 executes program instructions encoded in a modem driver 240. The modem driver 240 decodes the decrypted data and extracts control codes and/or user data. The modem driver 240 passes the control codes to the PHY hardware 220. In turn, the PHY hardware 220 configures the radio 230 based on the assigned time slot, frequency, and power level information contained in the control codes. See Patent Application, page 16, ll. 1-4. The processor complex 110 also executes program instructions for implementing the authentication agent 90. See Patent Application, page 15, ll. 6-10. The authentication agent 90 is periodically invoked to verify the authenticity of the modem driver 240. The authentication agent 90 is invoked in a privileged context. See Patent Application, page 16, line 11-15.

Independent claim 34 sets forth a method for identifying security violations in a computer system. The method includes executing a driver in a standard processing mode of a processing unit, transitioning the processing unit into a privileged processing mode, and authenticating the driver in the privileged processing mode. Claims 35-41 depend from claim 34.

For example, an operating system under which a computer 100 operates may include a timer that is used to periodically initiate an SMI to invoke the authentication agent 90. In another embodiment, security hardware including a secure timer may be included in the computer 100 for periodically invoking the authentication agent 90. For example, a restart timer 155 (see Figure 2), resident on the south bridge 150 may be used to periodically invoke the authentication agent 90 after a predetermined amount of time has elapsed. See Patent Application, page 17, line 17-21.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Appellant respectfully requests that the Board review and overturn the seven rejections present in this case. The following issues are presented on appeal in this case:

(A) Whether claims 1-2, 5-11, and 14-15 are anticipated by Beckert;

(B) Whether claims 3-4 and 12-13 are obvious over Beckert in view of Moore;

(C) Whether claims 16-17, 20-21, 23-29, and 32-33 are anticipated by Jain;

(D) Whether claims 18-19 and 31 are obvious over Jain in view of Moore;

(E) Whether claim 22 is obvious over Jain in view of Fleming;

(F) Whether claim 30 is obvious over Jain in view of Moore and further in view of Labatte; and

(G) Whether claims 34-41 are anticipated by Scherf.

VII. ARGUMENT

A. Legal Standards

An anticipating reference by definition must disclose every limitation of the rejected claim in the same relationship to one another as set forth in the claim. *In re Bond*, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (CCPA 1974). Second, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. That is, there must be something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination. *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561 (Fed. Cir. 1986). In fact, the absence of a suggestion to combine is dispositive in an obviousness determination. *Gambro Lundia AB v. Baxter Healthcare Corp.*, 110 F.3d 1573 (Fed. Cir. 1997). The mere fact that the prior art can be combined or modified does not make the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990); M.P.E.P. § 2143.01. Third, there must be a reasonable expectation of success.

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on Appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991); M.P.E.P. § 2142. A recent Federal Circuit case emphasizes that, in an obviousness situation, the prior art must disclose each and every element of the claimed invention, and that any motivation to combine or modify the prior art must be based upon a suggestion in the prior art. *In re Lee*, 61 U.S.P.Q.2d 143 (Fed. Cir. 2002). Conclusory statements regarding common knowledge and common sense are insufficient to support a finding of obviousness. *Id.* at 1434-35. Moreover, it is the claimed invention, as a whole, that must be considered for purposes of determining obviousness. A mere selection of various bits and pieces of the claimed invention from various sources of prior art does not render a claimed invention obvious, unless there is a suggestion or motivation in the prior art for the claimed invention, when considered as a whole.

B. Claims 1-2, 5-11, and 14-15 are not anticipated by Beckert.

Beckert describes a computer module 64 that may include a smart card reader 42 that accepts smart cards. The smart cards can be programmed to include encrypted driver identification information that a security system may use to authenticate the driver (*e.g.*, a person, such as an owner of the vehicle) of the vehicle. See Beckert, col. 9, ll. 36-54. In the Final Office Action, the Examiner notes that Beckert describes a multimedia audio driver 78. However, this is not the driver that is authenticated by the smart card. As discussed above, the smart card is used to authenticate the driver of the vehicle, *i.e.*, a human being. Thus, Appellants respectfully submit that Beckert does not describe or suggest a processing unit adapted to execute a driver, in the sense that the term "driver" is used in the present application. In particular, Beckert fails to describe or suggest a driver for interfacing with the peripheral device in a standard mode of operation and an authentication agent in a privileged mode of operation, as set forth in independent claim 1.

For at least the aforementioned reasons, Appellants respectfully submit that claims 1-2, 5-11, and 14-15 are not anticipated by Beckert and request that the Examiner's rejections of these claims under 35 U.S.C. § 102(b) be REVERSED.

C. Claims 3-4 and 12-13 are not obvious over Beckert in view of Moore.

As discussed above, Beckert fails to describe or suggest many features of the present invention. For example, Beckert fails to teach or suggest a driver for interfacing with the peripheral device in a standard mode of operation and an authentication agent in a privileged mode of operation, as set forth in independent claim 1. Moreover, Beckert fails to provide any suggestion or motivation to modify the prior art to arrive at Appellants claimed invention. In fact, Beckert is concerned with a completely different problem, *i.e.*, determining whether an authorized or unauthorized user of a vehicle is attempting to operate the vehicle. The Examiner relies upon Moore to describe the use of hashes and digests. However, Moore fails to remedy the fundamental deficiencies of the primary reference.

For at least the aforementioned reasons, Appellants respectfully submit that the Examiner has failed to make a *prima facie* case that the present invention is obvious over Beckert and Moore, either alone or in combination. Appellants request that the Examiner's rejections of claims 3-4 and 12-13 under 35 U.S.C. 103(a) be REVERSED.

D. Claims 16-17, 20-21, 23-29, and 32-33 are not anticipated by Jain.

Jain is concerned with preventing the transmission of authentication information to devices that are not directly connected to the transmitting device. Accordingly, Jain describes a network intermediate device 11 that may to authenticate end stations 10, 12, 13, 14, 15 that have a direct link to the network intermediate device in 11. See Jain, col. 4, ll. 11-43 and Figure 1. For example, a link beat on a link connected to a port of the network intermediate device 11 may be detected and then an encrypted initiate link test message may be sent to an end station across the link to determine participation of the end station. If participation of the end station is not detected then it is determined that there is no direct link and no authentication information is transmitted to the end station. If the end station does participate properly and the participation is detected, then it is decided that there is a direct link between the network device and the end station, and an authentication routine may be executed. See Jain, col. 5, ll. 18-33 and Figure 4.

However, the network intermediate device 11 performs both the link detection operation and the authentication routine in a single mode of operation. Thus, Appellants respectfully submit that Jain does not describe or suggest a processing unit adapted to execute a modem driver in a standard mode of operation and an authentication agent in a privileged mode of operation.

For at least the aforementioned reasons, Appellants respectfully submit that the present invention is not anticipated by Jain and request that the Examiner's rejections of claims 16-17, 20-21, 23-29, and 32-33 under 35 U.S.C. 102(e) be REVERSED.

E. Claims 18-19 and 31 are not obvious over Jain in view of Moore.

As discussed above, Jain fails to teach or suggest a processing unit adapted to execute a modem driver in a standard mode of operation and an authentication agent in a privileged mode of operation, as set forth in independent claim 16. Jain is also completely silent with regard to privileged modes of operation and therefore provides no suggestion or motivation to modify the prior art to arrive at Appellants claimed invention. The Examiner relies upon Moore to describe the use of hashes and digests. However, Moore fails to remedy the fundamental deficiencies of the primary reference.

For at least the aforementioned reasons, Appellants respectfully submit that the Examiner has failed to make a *prima facie* case that the present invention is obvious over Jain and Moore, either alone or in combination. Appellants request that the Examiner's rejections of claims 18-19 and 31 under 35 U.S.C. 103(a) be REVERSED.

F. Claim 22 is not obvious over Jain in view of Fleming.

Jain fails to teach or suggest a processing unit adapted to execute a modem driver in a standard mode of operation and an authentication agent in a privileged mode of operation, as set forth in independent claim 16. Jain is also completely silent with regard to privileged modes of operation and therefore provides no suggestion or motivation to modify the prior art to arrive at Appellants claimed invention. The Examiner relies upon Fleming to describe various control codes. However, Fleming fails to remedy the fundamental deficiencies of the primary reference.

For at least the aforementioned reasons, Appellants respectfully submit that the Examiner has failed to make a *prima facie* case that the present invention is obvious over Jain and Fleming, either alone or in combination. Appellants request that the Examiner's rejections of claim 22 under 35 U.S.C. 103(a) be REVERSED.

G. Claim 30 is not obvious over Jain in view of Moore and further in view of Labatte.

Jain fails to teach or suggest a processing unit adapted to execute a modem driver in a standard mode of operation and an authentication agent in a privileged mode of operation, as set forth in independent claim 16. Jain is also completely silent with regard to privileged modes of operation and therefore provides no suggestion or motivation to modify the prior art to arrive at Appellants claimed invention. The Examiner relies upon Moore to describe the use of hashes and digests and Labatte to describe storing a key in a BIOS. However, none of the secondary references remedy the fundamental deficiencies of the primary reference.

For at least the aforementioned reasons, Appellants respectfully submit that the Examiner has failed to make a *prima facie* case that the present invention is obvious over Jain, Moore, and Labatte, either alone or in combination. Appellants request that the Examiner's rejections of claim 30 under 35 U.S.C. 103(a) be REVERSED.

H. Claims 34-41 are not anticipated by Scherf.

Scherf describes a technique in which drivers in a system are allocated one data structure for each peripheral controlled by the driver. The drivers may then fill the data structures with information reflecting features and/or limitations of the attached devices. See Scherf, col. 4, ll. 1-5. If the device is a block device, the driver may insert the pointer to the driver's block hashing function in a block input/output hash function table. If the device is a character device, the driver may insert a pointer to the driver's character hashing function in a character input/output hash function table. See Scherf, col. 5, ll. 9-38.

However, Scherf is completely silent with regard to any particular operating modes of the system. Scherf is completely size with regard to a system that may operate in a standard mode of operation and a privileged mode of operation. Scherf therefore fails to teach or suggest executing a driver in a standard processing mode of a processing unit and transitioning the processing unit into a privileged processing mode, as set forth in claim 34. Scherf also fails to describe or suggest authenticating the driver in the privileged processing mode, as set forth in claim 34.

For at least the aforementioned reasons, Appellants respectfully submit that the present invention is not anticipated by Scherf and request that the Examiner's rejections of claims 34-41 under 35 U.S.C. 102(b) be REVERSED.

VIII. CLAIMS APPENDIX

The claims that are the subject of the present appeal – claims 1-41 – are set forth in the attached "Claims Appendix."

IX. EVIDENCE APPENDIX

There is no separate Evidence Appendix for this appeal.

X. RELATED PROCEEDINGS APPENDIX

There is no Related Proceedings Appendix for this appeal.

XI. CONCLUSION

In view of the foregoing, it is respectfully submitted that the Examiner erred in not allowing all claims pending in the present application, claims 1-41, over the prior art of record. The undersigned may be contacted at (713) 934-4052 with respect to any questions, comments or suggestions relating to this appeal.

Respectfully submitted,

Date: 4/25/06

Mark W. Sincell, Ph.D.
Reg. No. 52,226
WILLIAMS, MORGAN & AMERSON
10333 Richmond, Suite 1100
Houston, Texas 77042
(713) 934-7000
(713) 934-7011 (facsimile)

AGENT FOR APPELLANTS

CLAIMS APPENDIX

1. (Original) A computer system, comprising:

a peripheral device;

a processing unit adapted to execute a driver for interfacing with the peripheral device in a standard mode of operation and an authentication agent in a privileged mode of operation, wherein the authentication agent includes program instructions adapted to authenticate the driver.

2. (Original) The system of claim 1, wherein the authentication agent includes program instructions adapted to signal a security violation in response to a driver authentication failure.

3. (Original) The system of claim 1, wherein the authentication agent includes program instructions adapted to generate a hash of at least a portion of the driver, decrypt a digest associated with the driver, and compare the hash to the digest to authenticate the driver.

4. (Original) The system of claim 3, wherein the authentication agent includes program instructions adapted to decrypt the digest associated with the driver using a public key.

5. (Original) The system of claim 1, wherein the processing unit includes a timer adapted to generate an interrupt signal for invoking the authentication agent after a predetermined interval.

6. (Original) The system of claim 1, wherein the driver includes program instructions adapted to periodically invoke the authentication agent.

7. (Original) The system of claim 1, wherein the privileged mode of operation comprises a system management mode of operation.

8. (Original) The system of claim 1, wherein the driver includes program instructions adapted to issue a signal to the processing unit to initiate a change from the standard mode of operation to the privileged mode of operation.

9. (Original) The system of claim 8, wherein the signal comprises a system management interrupt.

10. (Original) The system of claim 1, further comprising a system basic input output system (BIOS) memory adapted to store the authentication agent.

11. (Original) The system of claim 10, wherein the processing unit is adapted to load the authentication agent from the system BIOS into a protected memory location during initialization of the computer system.

12. (Previously Presented) The system of claim 11, wherein the authentication agent includes program instructions adapted to generate a hash of at least a portion of the driver, decrypt a digest associated with the driver using a public key, and compare the hash to the digest

to authenticate the driver, and the system further comprises a system basic input output system (BIOS) memory adapted to store the public key.

13. (Previously Presented) The system of claim 1, wherein the authentication agent includes program instructions adapted to generate a hash of at least a portion of the driver, decrypt a digest associated with the driver using a public key, and compare the hash to the digest to authenticate the driver, and the peripheral device includes a memory device adapted to store the public key.

14. (Original) The system of claim 2, wherein the authentication agent includes program instructions adapted to prohibit further operation of the driver in response to identifying the security violation.

15. (Original) The system of claim 1, wherein the authentication agent includes program instructions adapted to prohibit further operation of the processing unit in response to identifying the security violation.

16. (Original) A communications system, comprising:

a physical layer hardware unit adapted to communicate data over a communications channel in accordance with assigned transmission parameters, the physical layer hardware unit being adapted to receive an incoming signal over the communications channel and sample the incoming signal to generate a digital received signal; and a processing unit adapted to execute a modem driver in a standard mode of operation and an authentication agent in a privileged mode of operation, wherein the standard mode driver includes program instructions adapted to extract control codes from the digital received signal and configure the physical layer hardware assigned transmission parameters based on the control codes, and the authentication agent includes program instructions adapted to authenticate the modem driver

17. (Original) The system of claim 16, wherein the authentication agent includes program instructions adapted to signal a security violation in response to a modem driver authentication failure.

18. (Original) The system of claim 16, wherein the authentication agent includes program instructions adapted to generate a hash of at least a portion of the modem driver, decrypt a digest associated with the modem driver, and compare the hash to the digest to authenticate the modem driver.

19. (Original) The system of claim 18, wherein the authentication agent includes program instructions adapted to decrypt the digest associated with the modem driver using a public key.

20. (Original) The system of claim 16, wherein the processing unit includes a timer adapted to generate an interrupt signal for invoking the authentication agent after a predetermined interval.

21. (Original) The system of claim 16, wherein the modem driver includes program instructions adapted to periodically invoke the authentication agent.

22. (Original) The system of claim 16, wherein the transmission assignments include at least one of a power level assignment, a frequency assignment, and a time slot assignment.

23. (Original) The system of claim 16, wherein the privileged mode of operation comprises a system management mode of operation.

24. (Original) The system of claim 16, wherein the modem driver includes program instructions adapted to issue a signal to the processing unit to initiate a change from the standard mode of operation to the privileged mode of operation.

25. (Original) The system of claim 24, wherein the signal comprises a system management interrupt.

26. (Original) The system of claim 16, wherein the processing unit comprises a computer.

27. (Original) The system of claim 26, wherein the computer includes:

a processor complex adapted to execute the program instructions in the modem driver and the authentication agent;

a bus coupled to the processor complex; and

an expansion card coupled to the bus, the expansion card including the physical layer hardware.

28. (Original) The system of claim 26, wherein the computer includes a system basic input output system (BIOS) memory adapted to store the authentication agent.

29. (Original) The system of claim 28, wherein the computer is adapted to load the privileged mode driver from the system BIOS into a protected memory location during initialization of the computer.

30. (Original) The system of claim 26, wherein the authentication agent includes program instructions adapted to generate a hash of at least a portion of the modem driver, decrypt a digest associated with the modem driver using a public key, and compare the hash to the digest to authenticate the modem driver, and the computer further comprises a system basic input output system (BIOS) memory adapted to store the public key.

31. (Original) The system of claim 27, wherein the authentication agent includes program instructions adapted to generate a hash of at least a portion of the modem driver, decrypt a digest associated with the modem driver using a public key, and compare the hash to the digest to authenticate the modem driver, and the expansion card includes a memory device adapted to store the public key.

32. (Original) The system of claim 17, wherein the authentication agent includes program instructions adapted to prohibit further operation of the modem driver in response to identifying the security violation.

33. (Original) The system of claim 16, wherein the authentication agent includes program instructions adapted to prohibit further operation of the processing unit in response to identifying the security violation.

34. (Original) A method for identifying security violations in a computer system, comprising:

executing a driver in a standard processing mode of a processing unit;

transitioning the processing unit into a privileged processing mode; and

authenticating the driver in the privileged processing mode.

35. (Original) The method of claim 34, further comprising signaling a security violation in response to a driver authentication failure.

36. (Original) The method of claim 34, wherein authenticating the driver includes:

generating a hash of at least a portion of the driver;

decrypting a digest associated with the driver; and

comparing the hash to the digest to authenticate the driver.

37. (Original) The method of claim 36, wherein decrypting the digest comprises decrypting the digest using a public key.

38. (Original) The method of claim 34, further comprising generating an interrupt signal for authenticating the driver in the privileged processing mode after a predetermined interval.

39. (Original) The method of claim 35, further comprising prohibiting further operation of the driver in response to identifying the security violation.

40. (Original) The method of claim 35, further comprising prohibiting further operation of the processing unit in response to identifying the security violation.

41. (Original) A system for identifying security violations, comprising:

means for executing a driver in a standard processing mode of a processing unit;

means for transitioning the processing unit into a privileged processing mode; and

means for authenticating the driver in the privileged processing mode.